Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) Computing apparatus comprising:

memory means storing the instructions of a secure process and an authentication process;

processing means arranged to control the operation of the computing apparatus including by executing the secure process and the authentication process;

user interface means arranged to receive user input and return to the user information generated by the processing means in response to the user input; and

interface means for receiving a removable primary token and communicating with the token, the token comprising a body supporting:

a token interface for communicating with the interface means;

a token processor; and

token memory storing token data including identity information for identifying the token and auxiliary token information identifying one or more authorised auxiliary tokens,

wherein the processing means is arranged to receive the identity information and the auxiliary token information from the primary token, authenticate the token using the authentication process and, if the token is successfully authenticated, permit a user to interact with the secure process via the user interface means,

and wherein the processing means is arranged to repeatedly authenticate the primary token and cause the computing platform to suspend interaction between the secure process and the user if authentication is not possible as a result of the removal of the primary token unless the primary token is replaced by an authorised auxiliary token.

2. (Original) Computing apparatus according to claim 1, arranged to generate information representing the integrity of the computing apparatus and transmit the

integrity information to the primary token, wherein the token processor is programmed to verify the integrity of the computing apparatus including by using the integrity information.

3. (Previously presented) Computing apparatus according to claim 1, wherein the authorised token is a cash token and the secure process is arranged to credit or debit the token.

4. (Previously presented) Computing apparatus according to claim 1, wherein the authorised token is a crypto token programmed to encrypt, decrypt or sign data, and the secure process is arranged to transmit data to the crypto token to be encrypted, decrypted or signed and receive encrypted, decrypted or signed data from the crypto token.

5. (Previously presented) Computing apparatus according to claim 1, arranged, only if the different token is an authorised auxiliary token, to allow the user to interact with the secure process.

6. (Previously presented) Computing apparatus according to claim 1, further comprising timer means programmed with a timeout period, wherein, in the event the different token is an authorised auxiliary token, the computing apparatus resets the timer and continues operation until the timeout period expires, after which time the computing apparatus suspends any interactions between the secure process and either or both the user and the authorised auxiliary token.

7. (Original) Computing apparatus according to claim 6, arranged to recommence said interactions in the event the authorised auxiliary token is replaced by the primary token and the computing apparatus is able to authenticate the primary token.

8. (Previously presented) Computing apparatus according to claim 1, arranged to permit interaction between the secure process and only one authorised auxiliary token after removal of the primary token.

9. (Previously presented) Computing apparatus according to claim 1, arranged to permit interaction between the secure process and more than one authorised auxiliary token after removal of the primary token.

10. (Previously presented) Computing apparatus according to claim 1, wherein the processing means comprises a main processing unit and a secure processing unit and the memory means comprises main memory and secure memory.

11. (Original) Computing apparatus according to claim 10, comprising a trusted device incorporating the secure processing unit and the secure memory, wherein the trusted device is programmed to authenticate the primary token repeatedly.

12. (Original) Computing apparatus according to claim 11, wherein the trusted device is arranged to acquire an integrity metric of the computing apparatus, and the primary token is arranged to use the integrity metric on at least one occasion to verify the integrity of the computing apparatus.

13. (Previously presented) Computing apparatus according to claim 1, wherein the primary token comprises a smart card, and the interface means is configured to receive a smart card.

14. (Previously presented) Computing apparatus according to claim 1, wherein the auxiliary token information is stored in a user profile.

15. (Original) A method of controlling computing apparatus to authenticate a user, comprising the steps:

the computing apparatus receiving a primary token of the user, the primary token

containing information suitable for authenticating the primary token and information relating to one or more authorised auxiliary tokens;

if the token is authentic, permitting the user to interact with one or more secure applications that may be executed by the computing platform;

at intervals, re-authenticating the primary token; and

if it is not possible to re-authenticate the primary token, suspending the interaction between the computing apparatus and the user unless the primary token has been replaced with an authorised auxiliary token.

16. (Original) A method according to claim 15, further comprising the steps:

the computing apparatus providing integrity metric information to the primary token;

the primary token using the integrity metric information to verify the integrity of the computing apparatus; and

if the primary token is unable to verify the integrity of the computing apparatus, suspending interaction between the computing apparatus and the user.

17. (Previously presented) A method according to claim 15, wherein the computing apparatus interaction with the authorised auxiliary token for a limited period of time.

18. (Previously presented) A method according to claim 15, wherein the computing apparatus only permits interaction with one authorised auxiliary token after removal of the primary token.

19. (Previously presented) A method according to claim 15, wherein the computing apparatus permits interaction with plural authorised auxiliary tokens after removal of the primary token.

20-21 (Canceled)

22. (Currently amended) Computing apparatus comprising:

one or more memories adapted to store the instructions of a secure process and an authentication process;

one or more processors arranged to control the operation of the computing apparatus including by executing the secure process and the authentication process;

a user interface arranged to receive user input and return to the user information generated by the one or more processors in response to the user input; and

a token reader interface for receiving and communicating with a removable token, the token having a token memory storing token data including identity information for identifying the token and auxiliary token information identifying one or more authorized auxiliary tokens,

wherein the one or more processors are arranged to receive the identity information and the auxiliary token information from a primary token received in the token reader interface, authenticate the primary token using the authentication process and, if the primary token is successfully authenticated, permit a user to interact with the secure process via the user interface, and wherein the one or more processors are ~~processing means is~~ arranged to repeatedly authenticate the primary token and cause the computing platform to suspend interaction between the secure process and the user if authentication is not possible as a result of the removal of the primary token unless the primary token is replaced by an authorized auxiliary token.

23. (Previously presented) Computing apparatus according to claim 22, wherein the primary token comprises a token processor and the one or more processors are arranged to generate information representing the integrity of the computing apparatus and transmit the integrity information to the primary token, wherein the token processor is programmed to verify the integrity of the computing apparatus including by using the integrity information.

24. (Previously presented) Computing apparatus according to claim 22, further comprising a timer programmed with a timeout period, wherein, in the event the different token is an authorized auxiliary token, the computing apparatus resets the timer and continues operation until the timeout period expires, after which time the

computing apparatus suspends any interactions between the secure process and either or both the user and the authorized auxiliary token.

25. (Previously presented) Computing apparatus according to claim 24, arranged to recommence said interactions in the event the authorized auxiliary token is replaced by the primary token and the computing apparatus is able to authenticate the primary token.

26. (Previously presented) Computing apparatus according to claim 22, wherein the one or more processors comprise a main processor and a secure processor and the one or more memories comprise a main memory and a secure memory.

27. (Previously presented) Computing apparatus according to claim 26, wherein said computer apparatus comprises a trusted device incorporating the secure processor and the secure memory, wherein the trusted device is programmed to authenticate the primary token repeatedly.

28. (Previously presented) Computing apparatus according to claim 27, wherein the trusted device is arranged to acquire an integrity metric of the computing apparatus, and the primary token is arranged to use the integrity metric on at least one occasion to verify the integrity of the computing apparatus.

29. (Previously presented) Computing apparatus according to claim 22, wherein the primary token comprises a smart card, and the token reader interface is configured to receive a smart card.